Merchant Liability for Security Breaches

June 2007
by Christine E. Lyon, William L. Stern

Related Practices:

- Financial Services Law
- Privacy and Data Security

In the world of security breach, the momentum has clearly shifted to the states, maybe this time for good. More than thirty-five states have already enacted breach-notification statutes. This trend may be unstoppable, with Congress unable to find common ground to settle on a national breach-notification standard.

If anything, the trend toward state control may be accelerating. In the past few months, following the mass data compromise of over 46 million credit and debit cards used at TJX Companies stores, the states appear ready to take things even further. At least six states—California, Connecticut, Illinois, Massachusetts, Minnesota, and Texas—may soon enact legislation that shifts to merchants *on a strict liability basis* the financial responsibility for security breaches occurring within their merchant systems.

Minnesota's Legislation

On May 16, the Minnesota Legislature became the first state to pass legislation that would make retailers and other merchants liable to banks for costs associated with data breaches, such as consumer notification and card replacement. The Minnesota bill (H.F. 1758) is notable, and not just because it came first. The bill passed the Minnesota Senate by a lopsided 63-1 vote and passed the House on a 104-27 vote. It is now on the Governor's desk awaiting signature.

The Minnesota measure is sweeping. It would prohibit merchants from retaining Track II data (information drawn from the magnetic stripe of a credit or debit card) and the personal identification number (PIN) or access code after completion of a credit or debit card transaction. For debit card transactions, merchants would be prohibited from storing such information for longer than 48 hours after completion of a transaction. If the merchant violated this anti-storage prohibition, a bank would have standing to sue the merchant to recover "the cost of reasonable actions undertaken" to respond to the breach, including the costs of cancelling and reissuing credit cards, closing and/or reopening accounts, stop-payment actions, unauthorized transaction reimbursements, and the providing of breach notification to account holders.

The Minnesota bill is also notable in its extra-territorial application. So long as a "person or entity" conducts "business in Minnesota that accepts an access device"—a card containing magnetic stripe data or a processor chip—"in connection with a transaction," that person or entity becomes automatically liable to any "financial institution" for the "reasonable costs" undertaken to protect the information of its cardholders. Note, the bill *doesn't* say that the merchant needed to be headquartered in Minnesota, that the breach had to have happened in Minnesota, or that the "financial institution" had to be located in Minnesota. The new rules apply to data breaches occurring on or after August 1, 2008.

Legislation Pending in Other States

Similar legislation has been introduced in at least five other states, including California, Connecticut, Illinois, Massachusetts, and Texas. Bills in Connecticut (S.B. 1089) and Illinois (S.B. 1675) are similar to Minnesota's. The Connecticut bill would amend that Connecticut's security breach

notification law to expressly impose liability on a person required to provide notice of a security breach for the costs of reasonable actions by banks as a result of the breach. Likewise, the Illinois bill would make a "data collector" under Illinois' security breach notification law liable to a financial institution for the costs or damages incurred relating to unauthorized access to credit card or debit card account data including, but not limited to, the cost of card replacement. Under S.B. 1675, the liability imposed on a data collector would be triggered on an unauthorized transaction on a credit card or debit card that is a result of a breach of security suffered by the data collector.

In California, A.B. 779 would amend the existing California data breach notification law to make merchants, other businesses, and government agencies liable to others, including banks, for reasonable costs associated with providing notifications as a result of a data breach. Reasonable costs include, but are not limited to, the cost of card replacement as a result of a breach. A.B. 779 would prohibit entities that accept credit cards, debit cards, or other payment devices from: storing, retaining, sending, or failing to limit access to payment card-related data, except as required for business, legal, or regulatory purposes; storing sensitive authentication data subsequent to authorization; or storing certain payment verification information.

On May 10, the Texas House unanimously passed a bill (H.B. 3222) that would amend its data breach notification law to allow banks to recover breach costs from merchants. Unlike the other states, Texas would codify the industry-imposed Payment Card Industry Data Security Standard and provide safe harbor from the proposed law for merchants in compliance with those industry standards. Under H.B. 3222, if a business in violation of this requirement is subject to a security breach, a financial institution may bring suit for actual damages arising from the violation.

Massachusetts—the home of TJX—started the ball rolling with the first retailer-liability bill (H. 213), but its fate is uncertain. Under this measure, a commercial entity would be liable to a bank for the costs of the bank's reasonable actions on behalf of the bank's customers as a direct result of a security breach including, but not limited to, the cost of card replacement.

Prognosis

Currently,liability for breach notification is a function of tort and contract law. Merchant and retailer liability to financial institutions is a function of the indemnity provisions in the contract (i.e., the merchant processing agreement) and network rules. But losses in the first instance are visited on card issuers, and issuers have had a difficult time recovering their losses from merchants. Principles such as privity, the "economic loss" doctrine, and other legal barriers have stood in the way of issuer recovery against merchants. *See, e.g., Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F.Supp.2d 183 (M.D. Pa. 2005).

If even one of these measures passes, the dynamic will change. A state like Minnesota could host data breach litigation that occurs anywhere in the nation so long as the merchant conducting business in that state accepts an "access device."

Still, the momentum begun in Minnesota may be hard to stem. We expect other states to amend their breach-notification laws to impose liability on merchants on a similar, strict-liability basis. If that happens, merchants will need to consider other risk management strategies, including buying insurance to cover damages resulting from a data breach. In fact, the Minnesota legislation may presage the beginning of a "products liability" model for handling liability following from mass security breaches, with strict liability being increasingly shifted to merchants, and merchants obtaining liability insurance to spread their risk.